UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA	**3:23-cr-** 85-MO
v.	**INFORMATION**
DANIEL JAMES JUNK,	**18 U.S.C. § 1349**
Defendant.	**Forfeiture Allegation**
	UNDER SEAL

THE UNITED STATES ATTORNEY CHARGES:

COUNT 1
(Conspiracy to Commit Wire Fraud)
(18 U.S.C. § 1349)

INTRODUCTION

1. From December 2019, through about March 2022, in the District or Oregon and elsewhere, defendant **DANIEL JAMES JUNK**, and others known and unknown to the United States Attorney, did agree to try to accomplish a common and unlawful plan to commit wire fraud. Specifically, defendant agreed with others to gain unlawful access to victims' cryptocurrency exchange accounts for the purpose of stealing cryptocurrency.

2. By way of background, a Subscriber Identity Module or Subscriber Identification Module ("SIM") is a technology used to identify and authenticate subscribers on mobile phone devices. A SIM swap scam is a cellular phone account takeover fraud that results in the routing

of a victim's incoming calls and text messages to a different phone. Once an individual swaps the SIM to link new identifiers to the same phone number, the individual may be able to access a victim's various personal accounts, including email accounts, cryptocurrency exchange accounts, and other accounts that use two-factor authentication.

MANNER AND MEANS

3. To carry out their material scheme to defraud, defendant and his coconspirators often searched online illicit and public databases to identify high-value victims who they believed owned large amounts of cryptocurrency with various cryptocurrency exchanges.

4. Defendant and his coconspirators then worked together to steal cryptocurrency from these victims. To do so, they arranged for victims' cellphone numbers to be swapped to SIM cards contained in cellular phones in the conspirators' possession.

5. Defendant and his coconspirators then used the victims' cellphone numbers to fraudulently gain access to the victims' email accounts and cryptocurrency exchange accounts. The conspirators would reset the passwords for the victims' accounts so that the conspirators could control the accounts.

6. Defendant and his coconspirators used information from the victims' accounts to access the victims' cryptocurrency exchange accounts and to unlawfully transfer, without authority, cryptocurrency owned by the victims to the conspirators themselves.

7. Defendant and his coconspirators would split the proceeds of the stolen cryptocurrency among themselves, often based on the particular roles that each member of the conspiracy performed.

8. Defendant personally used Wasabi Wallets and other techniques to mix cryptocurrency for the purpose of concealing and disguising his illicit gains.

9. During the course of the conspiracy, defendant and others used, and caused to be used, interstate wire communications to carry out or attempt to carry out an essential part of their scheme.

In violation of Title 18, United States Code, Section 1349.

FORFEITURE ALLEGATION

10. Upon conviction of the offense alleged in Count 1 of this Information, defendant **DANIEL JAMES JUNK** shall forfeit to the United States of America, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to said violation.

Dated: March 15, 2023

Respectfully submitted,

NATALIE K. WIGHT
United States Attorney

/s/ Quinn P. Harrington
QUINN P. HARRINGTON, OSB #083544
CRAIG J. GABRIEL, OSB #012571
SIDDHARTH DADHICH, TSB #24096310
Assistant United States Attorneys